

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-020779

(43)Date of publication of application : 23.01.1998

(51)Int.Cl.

G09C 1/00

H04L 9/08

(21)Application number : 08-177673

(71)Applicant : HITACHI INF SYST LTD

(22)Date of filing : 08.07.1996

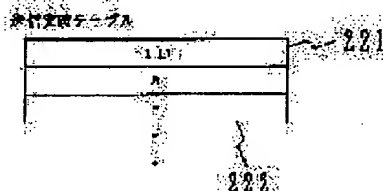
(72)Inventor : KOBORI MASAHIRO
SHIOMI YOSHIHIRO

(54) KEY CHANGING METHOD IN OPEN KEY CIPHER SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To change a key without inconvenience by decoding encoded data and electronic signed data smoothly with a past key so as to be able to obtain transmitter authorization after the key change of an open key cipher system.

SOLUTION: This key changing method is provided with a table 201 holding past secret keys, a table 211 holding past open keys, and a table 221 holding transmitted side data before the change of keys. An old open key is transmitted to the transmitted side to which data was actually sent before the change of the key, and the data before the change of the secret key and open key is decoded on the transmitted side to confirm a signature. In decoding processing on the receiving side, whether the received data can be decoded with a present secret key or not is judged, and in the negative case, the old secret key is retrieved from the secret key table 201 to decode the data with the retrieved old secret key.



LEGAL STATUS

[Date of request for examination] 25.09.1998

[Date of sending the examiner's decision of rejection] 28.11.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-20779

(43)公開日 平成10年(1998)1月23日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 B
		7259-5 J		6 3 0 F
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 B
				6 0 1 F

審査請求 未請求 請求項の数3 O L (全 8 頁)

(21)出願番号 特願平8-177673

(22)出願日 平成8年(1996)7月8日

(71)出願人 000152985

株式会社日立情報システムズ
東京都渋谷区道玄坂1丁目16番5号

(72)発明者 小堀 正裕

東京都渋谷区道玄坂一丁目16番5号 株式
会社日立情報システムズ内

(72)発明者 塩見 芳弘

東京都渋谷区道玄坂一丁目16番5号 株式
会社日立情報システムズ内

(74)代理人 弁理士 磯村 雅俊 (外1名)

(54)【発明の名称】 公開鍵暗号方式における鍵変更方法

(57)【要約】

【課題】公開鍵暗号方式の鍵変更後に、過去の鍵で暗号化したデータや電子署名したデータを円滑に復号し、送信者認証することができ、鍵の変更を不都合なく行う。

【解決手段】過去の秘密鍵を保持するテーブル201、過去の公開鍵を保持するテーブル211、および鍵変更以前の送信先データを保持するテーブル221を備え、鍵変更以前にデータを送信した実績のある送信先に旧公開鍵を送信し、それら送信先で秘密鍵および公開鍵の変更に前のデータを復号し、署名確認を行う。また、受信側の復号処理では、受信済みデータが現秘密鍵で復号可能であるか否かを判定し、不可能のとき旧秘密鍵を秘密鍵テーブル201を検索することにより、検索された旧秘密鍵でデータ復号を行う。

秘密鍵テーブル

利用期間	秘密鍵データ
*****
202	203

公開鍵テーブル

I D	利用期間	公開鍵データ
A	*****
212	213	214

送信実績テーブル

I D
A
222

【 特許請求の範囲】

【 請求項1 】 公開鍵暗号方式により不特定多数のコンピュータシステム間で暗号データ通信を行う場合の鍵変更方法において、

送信側および受信側のコンピュータシステムは、共に、過去の秘密鍵の履歴を保持する秘密鍵テーブル、受信した過去の公開鍵の履歴を保持する公開鍵テーブル、および暗号鍵変更以前にデータ送信した送信先IDを保持する送信実績テーブルを備え、

暗号鍵変更時には、上記送信側コンピュータシステムから上記送信実績テーブルの送信先IDを基に、該暗号鍵変更以前にデータ送信した送信先に旧公開鍵を送信し、上記受信側コンピュータシステムは、受信した旧公開鍵と上記各テーブルの内容とを用いて該暗号鍵変更以前のデータを復号するとともに、送信者の署名確認を行うことを特徴とする公開鍵暗号方式における鍵変更方法。

【 請求項2 】 前記旧公開鍵を受信した受信側コンピュータシステムは、他のコンピュータシステムから受信した全てのデータを格納するデータ格納ファイルを備え、該データ格納ファイルの送信側コンピュータシステムのIDおよび送信日付を参照して、これらと受信した上記旧公開鍵送信コンピュータシステムのIDおよび使用期間とが合致するものが存在した場合には、当該公開鍵を前記公開鍵テーブルに格納し、

合致するものが存在しない場合には、受信した上記旧公開鍵を破棄することを特徴とする請求項1に記載の公開鍵暗号方式における鍵変更方法。

【 請求項3 】 前記送信側コンピュータシステムは、現用の公開鍵でデータの暗号化処理、現用の秘密鍵で署名処理を行い、日付を付加して宛先に送信すると、

前記受信側コンピュータシステムは、受信したデータを復号する場合、前記秘密鍵テーブルの利用期間から、現時点での秘密鍵の利用開始日時と、上記受信データの送信日時とを比較し、該秘密鍵の利用開始日時が上記受信データの送信日時以後であった場合には、受信データの送信日時が上記秘密鍵テーブルにおける利用期間に含まれる秘密鍵データを検索し、検索された秘密鍵データを用いて上記受信データを復号するとともに、

送信者認証を行う場合、現用の公開鍵を前記公開鍵テーブルから取得し、該公開鍵の利用開始日時と、受信データの送信日時とを比較し、公開鍵の利用開始日時が当該データの送信日時以後であった場合には、送信日時が公開鍵テーブルにおける利用期間に含まれる公開鍵データを検索し、検索された公開鍵を用いて送信者認証を行うことを特徴とする請求項1に記載の公開鍵暗号方式における鍵変更方法。

【 発明の詳細な説明】

【 0001 】

【 発明の属する技術分野】 本発明は、コンピュータシステム間の公開鍵暗号方式による暗号データ通信を行う場

合の暗号化鍵の変更方法に関し、特に広域ネットワーク環境下における不特定多数との間の暗号通信時において、データの暗号化と送信者の認証に好適な公開鍵暗号方式における鍵変更方法に関する。

【 0002 】

【 従来の技術】 従来より、通信内容を保護するための暗号方式としては、『秘密鍵方式』と『公開鍵方式』とがある。このうち『秘密鍵方式』は、送信者と受信者が通信内容を暗号化あるいは解読するために、同一の暗号鍵情報を保有する方法であって、暗号化および復号するための情報は当事者間しか知らされていないために、情報の秘匿性は高いが、その反面、不特定多数を対象として通信する場合（放送や同報通信）には不向きである。これに対して、『公開鍵方式』は、不特定多数の相手に通信を行う場合に向いており、例えばインターネット上での商取引を支える技術として注目されている。公開鍵方式では、暗号化された通信内容を解読するための復号情報のみを秘密鍵として非公開とし、暗号化するための暗号化情報は公開鍵として公開される。なお、秘密鍵方式、公開鍵方式の従来文献としては、例えば『暗号化電子メールPEMの実装と例題』情報処理学会第46回全国大会（菊地、森下著）、および『暗号メールの仕組みとFJPEMの公開実験』平成6年5月31日（黒田、菊地、山口著）等がある。

【 0003 】 図9は、公開鍵方式の一般的な暗号化および復号方法を示す説明図である。図9において、送信者Aは受信者Bが公開したB公開鍵を用いて平文を暗号化し、暗号文を作成して受信者Bに送信する。一方、受信者Bは、自身のみが保有しているB秘密鍵を用いて受信した暗号文を復号して、元の平文に戻す。図10は、公開鍵方式をコンピュータネットワークシステムで使用する場合の構成図である。ここでは、公開鍵方式をインターネットに代表されるコンピュータネットワークシステムで使用する場合を示している。図10に示すように、暗号化するための公開鍵はサーバコンピュータに登録されており、誰からも参照、利用が可能である。一方、受信暗号文を復号するための秘密鍵は、各コンピュータで秘密に保持、管理されている。また、公開鍵暗号方式は、送信側の認証にも好適な暗号方法である。すなわち、送信側は自身の秘密鍵で認証メッセージを暗号化して、これを受信側に送信することにより、受信側は送信側の公開鍵で受信した認証メッセージを復号し、認証を行う。この場合、あるコンピュータシステムにおける秘密鍵および公開鍵は、数学的に対をなすものである。

【 0004 】

【 発明が解決しようとする課題】 しかしながら、秘密鍵および公開鍵の各暗号方式には、次のような問題点がある。まず、公開鍵暗号方式では、秘密鍵が各々のコンピュータシステムで秘密に保持されることを前提にしているため、仮にこの前提が崩壊した場合には、送信側が受

3

信側の公開鍵で暗号化した暗号文は、受信側の秘密鍵を保持する全ての者に復号可能になってしまうという問題がある。また、送信側が自身の秘密鍵で認証メッセージを暗号化して、これを受信側に送信し、受信側は送信側の公開鍵で認証メッセージの復号が可能であったとしても、送信側の証明とはなり得ないという問題もある。このような場合、当該コンピュータシステムの秘密鍵および公開鍵を変更する方法が必要となる。従来は、上述のような問題点があるため、広域ネットワーク環境下における不特定多数の暗号通信に公開鍵暗号方式を用いる場合、迅速に鍵を変更することは不可能であった。一般に、1対多数の暗号通信の場合には、事実上1対1の暗号通信と同等であるので、事前にコンピュータシステム間で同期をとることは容易であり、従って迅速に鍵を変更することは容易に考えられる。しかしながら、広域ネットワーク環境下では、不特定多数のコンピュータシステム間での秘密鍵および公開鍵の変更および更新の同期をとることは極めて困難であるため、安易に鍵を変更することができない。また、ある1時点を超えて鍵を変更した場合には、その1時点以前に受信した暗号文は新規秘密鍵では復号することができず、また1時点以前に受信した認証メッセージは新規公開鍵では認証不可能となる等の問題が生じる。そこで、本発明の目的は、これら従来の課題を解決し、過去の鍵で暗号化したデータおよび電子署名したデータを、鍵変更後に円滑に復号化および送信者認証を行い、迅速に公開鍵および秘密鍵の変更が可能であり、かつ鍵の変更を不都合なく行うことが可能な公開鍵暗号方式における鍵変更方法を提供することにある。

【 0005 】

【課題を解決するための手段】上記目的を達成するため、本発明の公開鍵暗号方式における鍵変更方法では、各コンピュータシステムに、過去の秘密鍵とその属性を保持するテーブル(秘密鍵テーブル)と、過去の公開鍵とその属性を保持するテーブル(公開鍵テーブル)と、鍵変更最終時点以前の送信実績とその属性に関するデータを保持するテーブル(送信実績テーブル)とを備え、暗号鍵を変更した時点で、送信側コンピュータシステムから送信実績テーブルを基に鍵変更最終時点以前の既送信先に旧公開鍵を送信し、受信側コンピュータシステムは、受信した旧公開鍵の属性により、その旧公開鍵の要または不要の判定を行い、旧公開鍵の蓄積または破棄を確定し、蓄積する場合には、旧公開鍵とその属性を保持するテーブル(公開鍵テーブル)に格納する。そして、格納された公開鍵に対応する旧秘密鍵を秘密鍵テーブルから検索することにより、検索された旧秘密鍵でデータを復号することができる。旧公開鍵の要、不要の判定には、上記公開鍵テーブルが参照される。これにより、秘密鍵および公開鍵を変更する以前のデータを復号化および署名確認することが可能となる。さらに、ローカルに

4

公開鍵を保持している場合にも、その変更のタイミングを自動的に通知することが可能となる。

【 0006 】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。図1は、本発明の一実施例を示す公開鍵暗号方式を適用するコンピュータシステムの全体構成図である。図1において、101はデータを送信する送信側コンピュータA、111はデータを受信する受信側コンピュータBである。また、102、112は後述(図2参照)するようなシステムで利用する各テーブルを格納した鍵管理ファイル、103、113は他のコンピュータシステムから受信したデータを格納するデータ格納ファイル、104、114はコンピュータAまたはBで動作する暗号化プログラム、105、115は鍵管理ファイル102、112の各テーブルを用いることにより、秘密鍵および公開鍵の管理および変更時における処理を行う鍵管理プログラムである。送信側および受信側の各コンピュータ101、111は、ともに過去の秘密鍵、鍵変更以前の送信先データをテーブルに保持しているので、このテーブルを参照することにより、暗号化鍵を変更する場合には、鍵変更以前にデータを送信した実績のある送信先へ旧公開鍵を送信し、受信側のコンピュータ111では、受信した旧公開鍵と、上記データ格納ファイル113および上記鍵管理ファイル112の各テーブルを参照して、秘密鍵および公開鍵を変更する以前のデータを復号化および署名確認する。これにより、過去の鍵で暗号化したデータおよび電子署名したデータを、鍵変更後に円滑に復号化し、かつ送信者認証することができる。

【 0007 】図2は、本発明における鍵管理ファイルを構成する各テーブルのフォーマット図である。図2において、201は鍵管理ファイルの内容のうち、コンピュータAにおける過去の秘密鍵を格納する秘密鍵テーブルであって、202は該当する秘密鍵の使用期間を年月日分秒で示し、203は当該秘密鍵のデータを示している。また、211は鍵管理ファイルの内容のうち、他のコンピュータシステムから受信した過去の公開鍵を格納する公開鍵テーブルであって、212は当該公開鍵を所有していたコンピュータのIDを示し、213は当該公開鍵の使用期間を年月日分秒で示し、214は当該公開鍵のデータを示している。また、221は鍵管理ファイルの内容のうち、鍵変更最終時点以前の送信先属性を格納する送信実績テーブルであって、222は送信先属性として送信先コンピュータのIDを示している。ここでは、コンピュータ101のIDをA、コンピュータ111のIDをBとしている。

【 0008 】図3は、旧公開鍵のフォーマットおよび受信データのフォーマットを示す図である。ここでは、コンピュータAが送信する旧公開鍵のフォーマット311と、コンピュータBの受信データ格納ファイルに格納さ

5

れている受信データフォーマット301が示されている。(a)の受信データフォーマットにおいて、302は送信先コンピュータのID、303は送信日時、304は受信済みのデータである。また、(b)の旧公開鍵フォーマットにおいて、312は公開したコンピュータのID、313はこの公開鍵が利用されていた期間、314は旧公開鍵データである。鍵変更時に、送信側コンピュータシステムAから旧公開鍵を送信すると、受信側コンピュータシステムBでは、受信した(b)の旧公開鍵フォーマットの利用期間と、(a)の受信データ格納

【0009】次に、鍵管理プログラムの鍵変更処理および旧公開鍵受信時処理の動作について説明する。図4は、コンピュータAで動作する鍵管理プログラムの鍵変更処理の動作フローチャートであり、図5は、コンピュータBで動作する鍵管理プログラムの旧公開鍵受信時処理の動作フローチャートである。図4に示すように、コンピュータAにおける鍵変更時には、ステップ401で旧秘密鍵をコンピュータAの秘密鍵テーブル201に追加して保存し、ステップ402で送信実績テーブル221を参照して、鍵変更最終時点以前のデータ送信先であるコンピュータ(ID222により識別)に対して旧公開鍵を送信する(ここでは、コンピュータBに送信)。次に、図5に示すように、ステップ501で旧公開鍵311を受信したコンピュータBは、ステップ502において、受信データ格納ファイル113に格納されている受信データフォーマット301の送信コンピュータのID302および送信日付303を参照して、受信した旧公開鍵送信コンピュータID312および使用期間313と合致するものが存在するか否か判定し、存在した場合には、ステップ503でコンピュータBの公開鍵テーブル211に追加し、保存する。追加、保存された旧公開鍵に対応する旧秘密鍵を秘密鍵テーブル201から検索して、検索した旧秘密鍵でデータを復号することができる。また、合致するものが存在しない場合には、ステップ504において即座に受信した旧公開鍵を破棄する。

【0010】次に、本発明における暗号化および復号の各処理について詳述する。図6は、コンピュータAで動作する暗号化プログラムの動作フローチャートであり、図7は、コンピュータBで動作する復号処理の動作フローチャートであり、図8は、図7における送信者認証処理の動作フローチャートである。いまコンピュータAからコンピュータBに対して暗号データを送信する場合、図6に示すように、ステップ601で現用の公開鍵を用いて暗号化処理を行い、ステップ602で現用の秘密鍵を用いて電子署名処理を行う。さらに、ステップ603でコンピュータAのIDおよび送信日付をデータ格納フ

6

イル301と同一フォーマットとなるように付加し、ステップ604で宛先に送信処理を行う。次に、コンピュータBにおいて、コンピュータAからの受信データを復号する場合、図7に示すように、ステップ701において受信データ格納ファイル113より該当データを参照し、ステップ702でコンピュータBにおける秘密鍵テーブル201の利用期間202から、現時点での秘密鍵の利用開始日時と、コンピュータB内の受信データ格納ファイル113に格納されたデータフォーマット301の該当データにおける送信日時303とを比較し、秘密鍵の利用開始日時が受信データの送信日時以後であった場合には、この秘密鍵では復号できない。そこで、この場合には、ステップ703で、受信データの送信日時がコンピュータB内の秘密鍵テーブル201における利用期間202に含まれる秘密鍵データ203を検索し、そのデータを参照してステップ704でこれを復号する。さらに、ステップ705において、現用の公開鍵で認証メッセージを復号することにより送信者認証処理を行う。

【0011】この送信者認証処理の詳細は、図8に示されている。図8のステップ801でコンピュータAの現在の公開鍵を公開鍵テーブル211から取得し、ステップ802でコンピュータAの現時点での公開鍵の利用開始日時と、コンピュータB内の受信データ格納ファイル113に格納された該当データフォーマット301の送信日時303とを比較し、公開鍵の利用開始日時が当該データの送信日時以後であった場合、この公開鍵では送信者認証を行うことはできない。そこで、ステップ803では、送信日時がコンピュータB内の公開鍵テーブル211におけるコンピュータIDがコンピュータAであり、利用期間213に含まれる公開鍵データ214を検索し、検索された公開鍵を用いて、ステップ805で送信者認証処理を行う。しかし、送信者認証可能なデータ、つまり受信済みデータ中に、受信公開鍵利用期間と送信日時とが一致するデータが受信データ格納ファイル113の格納済みデータ内になければ(ステップ804)、ステップ806で即座に公開鍵テーブル211内の当該公開鍵を破棄する。なお、ステップ802において、当該受信済みデータが現公開鍵で署名確認することが可能である場合には、ステップ805で現公開鍵を用いて送信者認証処理を行う。

【0012】このように、本発明においては、送信側および受信側のコンピュータシステムが共に過去の秘密鍵を保持するテーブルと鍵変更以前の送信先データを保持するテーブルを備え、送信側コンピュータが鍵を変更する時点で、これらのテーブルを基に鍵変更以前にデータを送信した実績のある送信先に旧公開鍵を送信し、秘密鍵および公開鍵を変更する以前のデータを復号化および署名確認する。これにより、公開鍵暗号方式において、過去の鍵で暗号化したデータおよび電子署名したデータ

50

を、鍵変更後に円滑に復号化および送信者認証を行うことができる。その結果、鍵の変更を不都合なく行うことができる。

【0013】

【発明の効果】以上説明したように、本発明によれば、過去の鍵で暗号化したデータおよび電子署名したデータを、鍵変更後に円滑に復号化および送信者認証を行うので、迅速に公開鍵および秘密鍵の変更が可能であり、かつ鍵の変更を不都合なく行うことが可能である。

【図面の簡単な説明】

【図1】本発明の一実施例を示す公開鍵暗号方式を適用したコンピュータシステムの全体構成図である。

【図2】図1における鍵管理ファイルに格納されたテーブルフォーマット図である。

【図3】図1におけるデータ格納ファイルに格納されている受信データフォーマットおよび鍵を変更したコンピュータが送信する旧公開鍵のフォーマットの図である。

【図4】図1における鍵管理プログラムの鍵変更処理の動作フローチャートである。

【図5】図1における鍵管理プログラムの旧公開鍵受信時処理の動作フローチャートである。

【図6】図1における暗号化プログラムの動作フローチャートである。

【図7】本発明における復号処理の動作フローチャートである。

【図8】図7における送信者認証処理の動作フローチャートである。

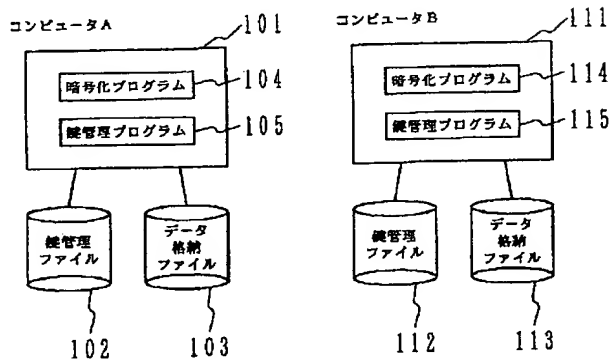
【図9】従来の公開鍵暗号方式の暗号化および復号の処理方法を示す全体構成図である。

【図10】従来の公開鍵暗号方式をコンピュータネットワークシステムで使用する場合の機能ブロック図である。

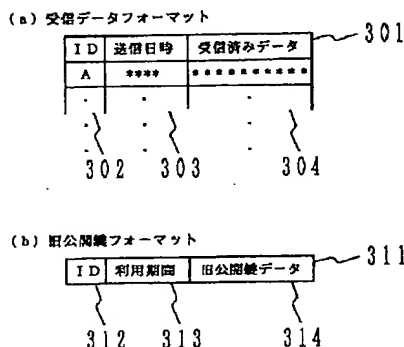
10 【符号の説明】

101…データ送信側コンピュータA、111…データ受信側コンピュータB、
102、112…鍵管理ファイル、103、113…データ格納ファイル、104、114…暗号化プログラム、105、115…鍵管理プログラム、201…秘密鍵テーブル、202…秘密鍵の利用期間、203…秘密鍵データ、
211…公開鍵テーブル、212…コンピュータのID、213…公開鍵の利用期間、214…公開鍵データ、221…送信実績テーブル、222…送信先コンピュータのID、301…受信データフォーマット、311…旧公開鍵のフォーマット。

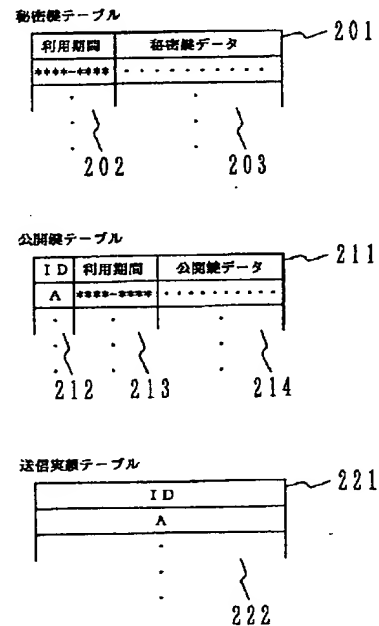
【図1】



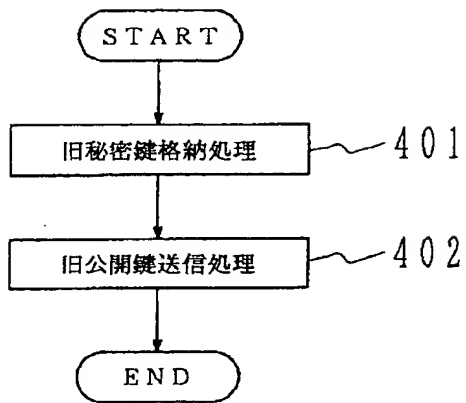
【図3】



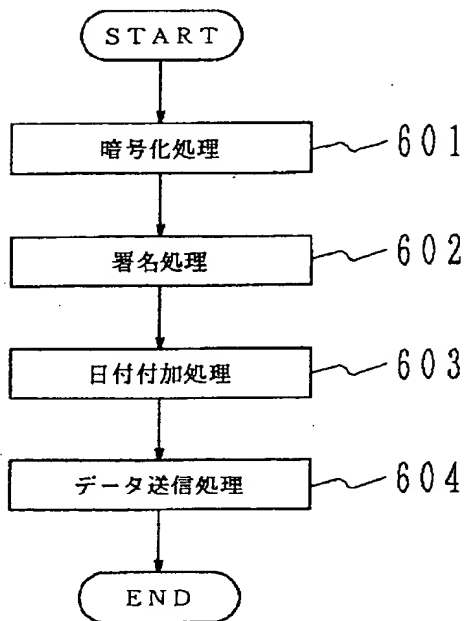
【図2】



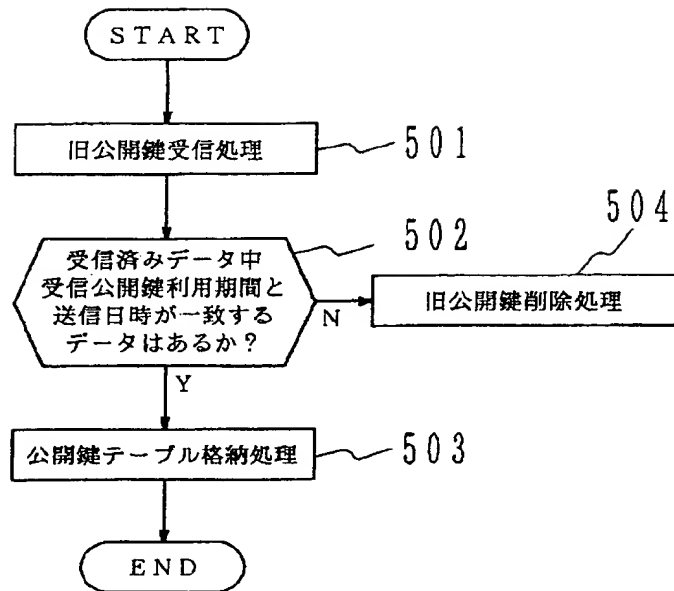
【 図4 】



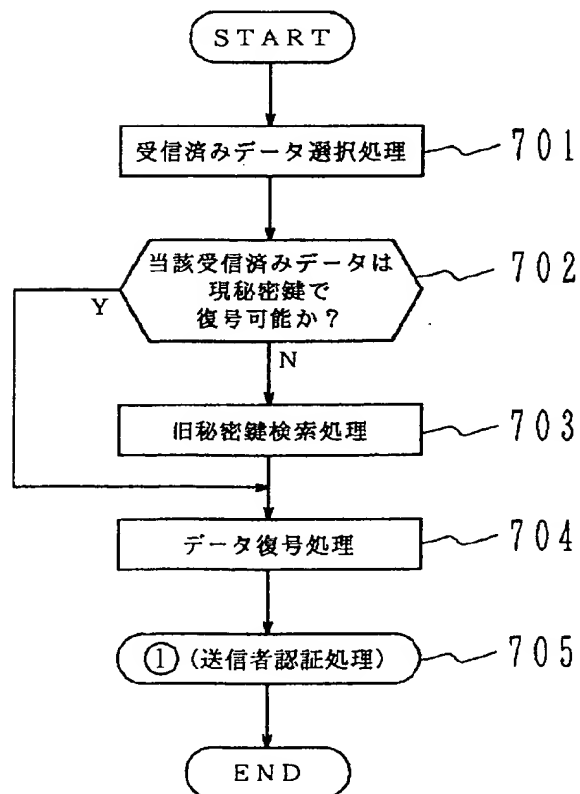
【 図6 】



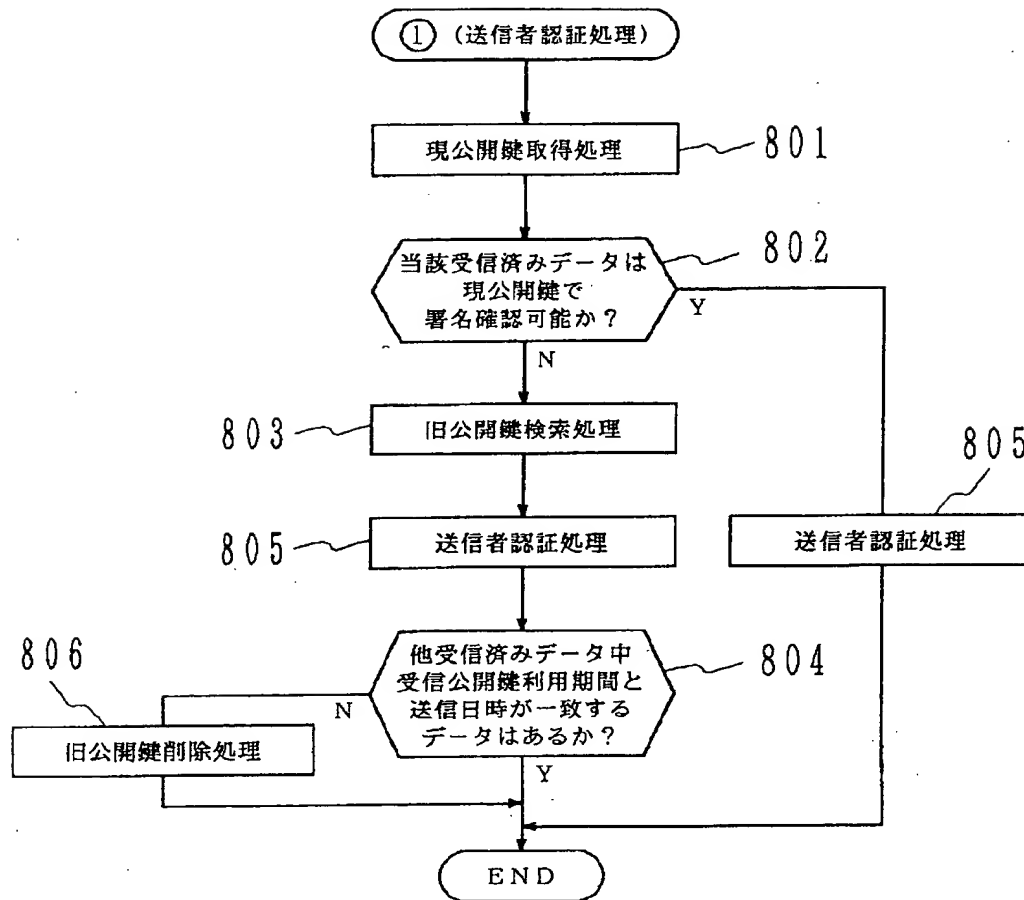
【 図5 】



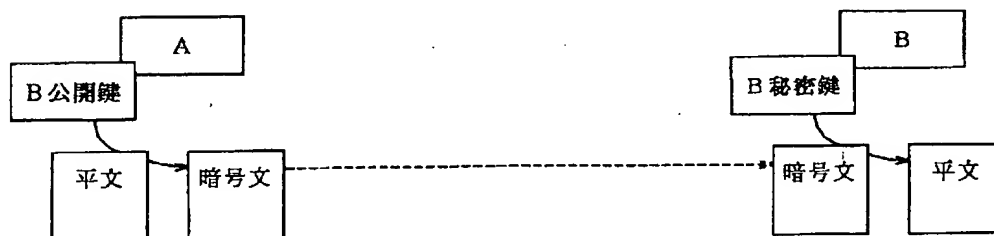
【 図7 】



【 図8 】



【 図9 】



【 図10 】

